Before the
Subcommittee on Commerce, Trade, and Consumer Protection
of the
House Energy & Commerce Committee

Hearing on
Protecting Consumer's Data: Policy Issues Raised by Choice Point
March 15, 2005

Kurt P. Sanford
President and CEO
U.S. Corporate and Federal Government Markets
LexisNexis

Introduction

Good morning. My name is Kurt Sanford. I am the Chief Executive Officer for Corporate and Federal Markets at LexisNexis, a division of Reed Elsevier Inc. On behalf of LexisNexis, I appreciate the opportunity to be here today to discuss the important public policy issues associated with the protection of consumer information, cybercrime, and identity theft. LexisNexis commends the Subcommittee for its leadership on these important issues.

LexisNexis is a leading provider of authoritative legal, public records, and business information. Today, over three million professionals—lawyers, law enforcement officials, government agencies, financial institutions and others—subscribe to the LexisNexis services. Government agencies at all levels, businesses, researchers, and others rely on LexisNexis to carry out important functions in our society. LexisNexis Risk Management unit plays a vital role in supporting government and business customers who use our information services for a variety of important uses.

The following are examples of some of the important ways in which the services of LexisNexis are used by customers:

- ***Prevent identity theft and fraud –*** Banks and other financial institutions routinely rely on personally identifying information contained in LexisNexis' databases to verify the identities of individuals and businesses and prevent identity theft and fraud. For example, LexisNexis has partnered with the American Bankers Association to enable banks and other customers to prevent money laundering and ensure compliance with applicable laws by helping the banks determine if they are doing business with legitimate businesses and consumers. The use of this information by financial

institutions to verify and validate information on prospective customers is critical to the success of that program. With the help of LexisNexis, major banks and bank card issuers have experienced significant reductions in dollar losses due to fraud, holding down costs charged to consumers. Special investigation units of insurance companies have experienced similar successes through the use of information in our databases.

- ***Locating suspects and helping make arrests –*** Many federal, state and local law enforcement agencies rely on LexisNexis to help them locate criminal suspects and to identify witnesses to a crime. For example, Seisint products were used during the course of the D.C. sniper investigation and helped lead to the arrest of the suspects.

- ***Preventing and investigating terrorist activities*** – Information service providers like LexisNexis offer important tools in the battle against terrorism. Our data, technology, and policy expertise has been instrumental in detecting and preventing terrorist activities.

- ***Locating and recovering missing children and assisting in the enforcement of child support obligations –*** For many years, LexisNexis has partnered with the National Center for Missing and Exploited Children to help that organization locate missing and abducted children. Locating a missing child within the first 48 hours is critical to success in the recovery effort. The NCMEC has told us that information from LexisNexis has been critical in the Center's successful recovery of many children. In addition, public and private agencies rely on information provided by LexisNexis to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. The Association for Children for

Enforcement of Support (ACES), a private child support recovery organization, has had tremendous success in locating nonpaying parents using LexisNexis.

LexisNexis is committed to the responsible use of personally identifiable information and to the protection of consumer privacy. We share the Subcommittee's concern about the potential misuse of this information to commit identity theft and fraud. We look forward to sharing our views on possible ways to further enhance information security and address the growing problems of cybercrime and identity theft.

The Pending Investigation of the Seisint Security Incidents, LexisNexis' Response and Cybercrime Implications

Before I proceed, I would like to take a few minutes to discuss the data security incidents we recently discovered at Seisint, the information company we acquired last September.

As part of LexisNexis integration of Seisint, we have been conducting a thorough review of the company's verification, authorization, and security procedures and policies. During that process, a LexisNexis integration team became aware of some billing irregularities within several customer accounts. Upon further investigation, the team detected within those accounts some unusual usage patterns. The team then informed senior management and we contacted the United States Secret Service. The U.S. Secret Service was notified because of its well-known expertise in investigating cybercrime and because of its national High Tech Crime Task Force, in which LexisNexis participates.

The incidents are still being investigated, but it appears that cybercriminals compromised IDs and passwords of legitimate Seisint customers and used those IDs and passwords to access certain Seisint databases. The information accessed was limited to public record information and certain identifying information, such as social security numbers and driver's license information. No personal financial, credit, or medical information was involved because Seisint does not collect or distribute information of this type.

We take these incidents very seriously. LexisNexis has long been committed to the protection of consumer privacy and security. We sincerely regret that these criminals were able to fraudulently access this information. We further regret any adverse impact that this crime may have upon the individuals whose information was accessed. We have already begun to take steps to assist individuals whose information may have been accessed. First, based on the investigation to date, we are in the process of notifying approximately 32,000 individuals whose personal information may have been accessed and we expect to complete mailing notices by March 16. Second, we will be providing all affected individuals with a consolidated report containing information from the three major credit bureaus. Third, we will be providing credit monitoring service for one year. Fourth, for those individuals who do become victims of fraud, we will provide them with ID theft counselors to help them through the process of clearing their credit reports of any information from related fraudulent activity.

Because this is an ongoing law enforcement investigation, the U.S. Secret Service has advised us that discussing additional details could compromise its investigation.

The Types of Measures Used To Safeguard Identifiable Information

LexisNexis has long recognized the importance of undertaking extensive measures to protect the information in our databases and has in place a comprehensive security program. Maintaining security is a not a static process, but rather involves continuously evaluating and adjusting our security program in light of technological advances and perceived or real threats.

LexisNexis has physical, administrative, and technical measures to protect the security of information it maintains on its services. Our data facilities are physically secure. Comprehensive monitoring capabilities exist throughout these facilities. These capabilities include interior and exterior cameras and a badge-access system with badge readers at all key entry points in the building, which are monitored 24x7 by on-site security guards.

Administratively, we limit access to data center facilities to those individuals with job-related needs and management authorization. To prevent employee misuse of our systems, we have policies and procedures in place to monitor usage and address policy abuses through clearly stated measures, up to and including termination.

In addition, we limit a customer's access to information, including sensitive information, in LexisNexis products according to the purposes for which they seek to use the information. Our Chief Privacy Officer and Privacy and Policy Review Board work together to ensure that LexisNexis has strong privacy policies in place to help protect the privacy of information contained in our databases. We also undertake regular assessments by independent third parties of both our privacy and security practices. In addition, because we recognize that the

success of our security program depends on our employees, we have developed training programs on privacy and security policies and practices.

We use a multi-layered technical approach to securing data and applications. Preventive and detective technologies are deployed to mitigate risk throughout the network and system infrastructure and serve to thwart potentially malicious activities.

In addition to the security safeguards outlined above, LexisNexis has a multi-layer process in place to screen potential customers to ensure that only legitimate customers have access to sensitive information contained in our systems. Our procedures include a detailed authentication process to determine the validity of business licenses, memberships in professional societies and other credentials. We also authenticate the documents provided to us to ensure they have not been tampered with or forged.

We have verification procedures in place to vet customers prior to providing them with access to sensitive information. Customers requesting access to sensitive information must go through a multi-step application and approval process. Only those customers with a permissible purpose under federal law are granted access to sensitive data such as driver's license information and social security numbers. In addition, customers are required to make express representations and warranties regarding access and use of sensitive information.

LexisNexis plans to further restrict access to the most sensitive data elements, Social Security Numbers and Driver's License Numbers, by extending LexisNexis current more restrictive SSN truncation policy to its recently acquired Seisint business and is adding a policy to include the masking of DLNs. These steps are part of the on-going review that LexisNexis

has been conducting on security practices, authorization and verification procedures and privacy policies across its businesses.

We have also accelerated our program to review and integrate verification and security procedures at LexisNexis and Seisint. Specifically, LexisNexis is in the process of:

- Enhancing ID and password administration procedures;
- Enhancing security requirements applied to our customers; and
- Working with law enforcement and outside consultants to establish new procedures and techniques to thwart criminal activity.

The Types of Information Maintained by LexisNexis

The information maintained by LexisNexis falls into the following three general classifications: public record information, publicly available information, and non-public information. I briefly describe each below.

Public record information. Public record information is information originally obtained from government records that are available to the public. Land records, court records, and professional licensing records are examples of public record information collected and maintained by the government for public purposes, including dissemination to the public.

Publicly available information. Publicly available information is information about an individual that is available to the general public from non-governmental sources. Some examples of these non-governmental sources are telephone directories, newspaper reports, and other general-distribution publications.

Non-public information. Non-public information is information about an individual that is not obtained directly from public record information or publicly available information. This information comes from proprietary or non-public sources. Non-public data maintained by LexisNexis consists primarily of information obtained from either motor vehicle records or so-called credit header data. Credit header data is the non-financial individual identifying information located at the top of a credit report, such as name, current and prior address, listed telephone number, social security number, and month and year of birth.

Laws Governing LexisNexis Compilation and Dissemination of Identifiable Information

There are a wide range of federal and state privacy laws to which LexisNexis is subject in the collection and distribution of personally identifiable information. These include:

The Gramm-Leach-Bliley Act. Social security numbers are one of the two most sensitive types of information that we maintain in our systems and credit headers are the principal commercial source of social security numbers. Credit header data is obtained from consumer reporting agencies.[1] Starting in July 2001, the compilation of credit header data is subject to the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801 *et seq*., and information subject to the GLBA cannot be distributed except for purposes specified by the Congress, such as the prevention of fraud. For credit header data compiled prior to July 2001, the dissemination of this

[1] Consumer reporting agencies are governed by the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 *et seq*. Some information services, such as Seisint's Securint service and LexisNexis PeopleWise, also are subject to the requirements of the FCRA.

information is subject to a set of industry-developed principles endorsed and enforced by the Federal Trade Commission.

Driver's Privacy Protection Act. The compilation and distribution of driver's license numbers and other information obtained from driver's licenses are subject to the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. §§ 2721 *et seq*., as well as state laws. Information subject to the DPPA cannot be distributed except for purposes specified by the Congress, such as fraud prevention, insurance claim investigation, and the execution of judgments.

Telecommunications Act of 1996. Telephone directories and similar publicly available repositories are a major source of name, address, and telephone number information. The dissemination of telephone directory and directory assistance information is subject to the requirements of the Telecommunications Act of 1996, as well as state law.

FOIA and other Open Records Laws: Records held by local, state, and federal governments are another major source of name, address, and other personally identifiable information. The Freedom of Information Act, state open record laws, and judicial rules govern the ability of LexisNexis to access and distribute personally identifiable information obtained from government agencies and entities. *See, e.g.,* 5 U.S.C. § 552.

Other laws:

Unfair and Deceptive Practice Laws: Section 5 of the Federal Trade Commission Act, and its state counterparts, prohibit companies from making deceptive claims about their privacy and security practices. These laws have served as the basis for enforcement actions by the

Federal Trade Commission and state attorneys general for inadequate information security practices. The consent orders settling these enforcement actions typically have required companies to implement information security programs that conform to the standards set forth in the GLBA Safeguards Rule, 16 C.F.R. Part 314.

Information Security Laws: A growing body of state law imposes obligations upon information service providers to safeguard the identifiable information they maintain. For example, California has enacted two statutes that require businesses to implement and maintain reasonable security practices and procedures and, in the event of a security breach, to notify individuals whose personal information has been compromised. *See* California Civil Code §§ 1798.81.5, 1798.82-84.

Legislative Measures LexisNexis Supports

We recognize that additional legislation may be necessary to address the growing problem of cybercrime and identity theft. LexisNexis supports the following legislative approaches:

Data Security Breach Notification. Consistent with the proposals outlined by FTC Chairman Majoras in her testimony before the Senate Banking Committee last week, we support requiring notification in the event of a security breach where there is substantial risk of harm to consumers. We share the concerns that Chairman Majoras raised in her testimony about ensuring that there is an appropriate threshold for when customers actually would benefit from receiving notification, such as where the breach is likely to result in misuse of customer information. In addition, we believe that it is important that any such proposal contain federal

preemption to insure that companies can quickly and effectively notify consumers and not struggle with complying with multiple, potentially conflicting and inconsistent state laws.

Adoption of Data Security Safeguards for Information Service Providers Modeled After the GLBA Safeguard Rule. LexisNexis would support the proposal outlined by Chairman Majoras whereby the types of security protections required by the Safeguard Rule of the GLBA would be applicable to information service providers that are not themselves "financial institutions" as defined under GLBA.

Increased penalties for identity theft and other cybercrimes and increased resources for law enforcement. LexisNexis strongly encourages legislation that imposes more stringent penalties for identity theft and other cybercrimes. Additionally, consumers and industry alike would benefit from enhanced training for law enforcement and an expansion of the resources available to investigate and prosecute the perpetrators of identity theft and cybercrime. Too many of our law enforcement agencies do not have the resources to neutralize these high-tech criminals.

It is critical that any legislation being considered ensure that legitimate businesses, government agencies, and other organizations continue to have access to identifying information that they depend on for important purposes including fraud detection and prevention, law enforcement, and other critical applications. Moreover, legislation must strike the right balance between protecting privacy and ensuring continued access to critically important information that is provided through information service providers.

Conclusion

Mr. Chairman, members of the Subcommittee, thank you again for the opportunity to testify before you today. LexisNexis is committed to:

- Developing effective products involving the responsible use of personally identifiable information to support law enforcement, government, and responsible businesses ;
- Safeguarding consumer privacy; and
- Protecting the security of our data systems.

We look forward to working with you as you develop proposals to help protect consumers and help fight cybercrime and identity theft.